

# **Passive Reconnaissance Scan Report**

**Scan target : bjnetworksolution.xyz  
(66.29.153.49)**

**Date of recon: 26 Nov 2025**

**Cybersecurity Analyst  
Bolaji Bakare**

**Scope: bjnetworksolution.xyz and publicly  
resolvable subdomains only (passive OSINT).**

**Out-of-scope: Active vulnerability exploitation,  
authenticated access and service disruption,  
rate-aggressive crawling.**

## Executive Summary

- The target domain resolves and serves a public website with recent content.
- This report enumerates: WHOIS/RDAP, authoritative DNS data, HTTPS surface (at a high level), presence of a WAF/CDN (fingerprinted passively) and open-source footprint across common OSINT sources.
- No intrusive scans were performed; all findings are from passive lookups and single request fetches of public pages.

## Methodology (Passive Only)

### Tools & Modes

- **whois / RDAP:** Registration & registrar metadata
- **dig, host, dnsrecon:** Passive DNS lookups (A/AAAA, NS, MX, TXT/SOA/CAA where present) via public resolvers.
- **wafw00f:** Single HTTP(S) request fingerprint (headers/body markers) to infer WAF/CDN; *no evasion, no burst.*
- **SpiderFoot (SF):** *Passive modules only* (DNS, CT logs, WHOIS, netblocks, leak/site mentions, social).
- **Wapiti:** *Listing only* and passive banner/headers check.
- **OSINT Framework:** As a directory to guide passive pivoting, CT logs, public paste sites, reputation lists, and search operators.

## Findings

### 3.1 Public Web Presence (Landing Page)

Site reachable: <https://bjnetworksolution.xyz/> returns content; homepage shows recent posts.

```
(bjnetwork㉿kali)-[~]
$ ping google.com
PING google.com (172.253.63.113) 56(84) bytes of data.
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=1 ttl=255 time=
104 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=2 ttl=255 time=
31.6 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=3 ttl=255 time=
59.2 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=4 ttl=255 time=
330 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=5 ttl=255 time=
213 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=6 ttl=255 time=
124 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=7 ttl=255 time=
63.2 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=8 ttl=255 time=
91.9 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=9 ttl=255 time=
47.4 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=10 ttl=255 time=
=221 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=11 ttl=255 time=
37.0 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=12 ttl=255 time=
=57.2 ms
64 bytes from bi-in-f113.1e100.net (172.253.63.113): icmp_seq=13 ttl=255 time=
```

### 3.2 Registration (WHOIS)

**Registrar / Dates:** Use ICANN RDAP as the primary source of truth (GDPR-redacted where applicable).

Query via ICANN Lookup and registrar RDAP.

```
└─(bjnetwork㉿kali)-[~]
└─$ whois bjnetworksolution.xyz
Domain Name: BJNETWORKSOLUTION.XYZ
Registry Domain ID: D621711462-CNIC
Registrar WHOIS Server: whois.porkbun.com
Registrar URL: https://porkbun.com/
Updated Date: 2025-11-26T05:52:04.0Z
Creation Date: 2025-11-26T05:51:42.0Z
Registry Expiry Date: 2026-11-26T23:59:59.0Z
Registrar: Porkbun, LLC
Registrar IANA ID: 1861
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferP
rohibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
bited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Name Server: CURITIBA.NS.PORKBUN.COM
Name Server: FORTALEZA.NS.PORKBUN.COM
Name Server: MACEIO.NS.PORKBUN.COM
Name Server: SALVADOR.NS.PORKBUN.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@porkbun.com
Registrar Abuse Contact Phone: +1.8557675286
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-11-27T00:14:28.0Z <<<
```

**Name servers:** Capture NS from RDAP and confirm against dig NS.

```
└─(bjnetwork㉿kali)-[~]
└─$ dig bjnetworksolution.xyz

; <>> DiG 9.20.11-4+b1-Debian <>> bjnetworksolution.xyz
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 24678
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;bjnetworksolution.xyz.      IN      A

;; ANSWER SECTION:
bjnetworksolution.xyz.  8      IN      A      44.230.85.241
bjnetworksolution.xyz.  8      IN      A      52.33.207.7

;; Query time: 80 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Wed Nov 26 19:15:18 EST 2025
;; MSG SIZE  rcvd: 82
```

### 3.3 DNS Surface (A/AAAA, NS, MX, TXT, SOA, CAA)

- **Records collected passively:**
  - A/AAAA for apex and www.
  - NS to identify hosting/DNS provider.
  - MX for mail handling (and whether any third-party service is used).
  - TXT for SPF/DMARC/DKIM indicators.

SOA for primary NS and serial.

```
(bjnetwork㉿kali)-[~]
└─$ dnsrecon -d bjnetworksolution.xyz
[*] std: Performing General Enumeration against: bjnetworksolution.xyz ...
[*] Wildcard resolution is enabled on this domain
[*] It is resolving to uixie.porkbun.com
[*] It is resolving to 44.230.85.241
[*] It is resolving to 52.33.207.7
[*] All queries will resolve to this list of addresses !!
[*] DNSSEC is not configured for bjnetworksolution.xyz
      SOA curitiba.ns.porkbun.com 173.245.58.37
      SOA curitiba.ns.porkbun.com 2400:cb00:2049:1::adf5:3a25
      NS fortaleza.ns.porkbun.com 162.159.8.140
      Bind Version for 162.159.8.140 "2025.11.1"
      NS fortaleza.ns.porkbun.com 2400:cb00:2049:1::a29f:88c
      NS maceio.ns.porkbun.com 162.159.11.180
      Bind Version for 162.159.11.180 "2025.11.1"
      NS maceio.ns.porkbun.com 2400:cb00:2049:1::a29f:bb4
      NS salvador.ns.porkbun.com 162.159.10.150
      Bind Version for 162.159.10.150 "2025.11.1"
      NS salvador.ns.porkbun.com 2400:cb00:2049:1::a29f:a96
      NS curitiba.ns.porkbun.com 173.245.58.37
      Bind Version for 173.245.58.37 "2025.11.1"
      NS curitiba.ns.porkbun.com 2400:cb00:2049:1::adf5:3a25
      MX mx3.zoho.com 136.143.183.44
      MX mx.zoho.com 136.143.183.44
      MX mx2.zoho.com 136.143.183.44
[*] A bjnetworksolution.xyz 44.230.85.241
```

### **3.5 Web Application Firewall**

- **Passive approach:**

The image shows a terminal window with the following content:

```
[*] Checking https://google.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

The title bar of the terminal window reads: "[(bjnetwork㉿kali)-[~]] \$ wafw00f google.com". The main area of the terminal displays a stylized dog head logo with the word "WOOF!" inside its mouth, followed by several error codes and their corresponding red X icons:

- 404 Hack Not Found
- 405 Not Allowed
- 403 Forbidden
- 502 Bad Gateway
- 500 Internal Error

Below the errors, the text "~ WAFW00F : v2.3.1 ~" and "The Web Application Firewall Fingerprinting Toolkit" is displayed.

### 3.6 OSINT: Mentions, Accounts, and Exposure

- SpiderFoot (passive modules):

**DNS/Hosts:** Passive resolution of subdomains from CT/DNS.

```
(bjnetwork㉿kali)-[~]
$ spiderfoot -l 127.0.0.1:5000
2025-11-26 19:22:08,170 [INFO] sf : Starting web server at 127.0.0.1:5000 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000/
*****

2025-11-26 19:22:08,184 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

## New Scan

**Scan Name**

bj-work-project

**Scan Target**

bjnetworksolution.xyz

ⓘ Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

**Domain Name:** e.g. *example.com*  
**IPv4 Address:** e.g. *1.2.3.4*  
**IPv6 Address:** e.g. *2606:4700:4700::1111*  
**Hostname/Sub-domain:** e.g.  
*abc.example.com*  
**Subnet:** e.g. *1.2.3.0/24*  
**Bitcoin Address:** e.g.  
*1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R*

**E-mail address:** e.g. *bob@example.com*  
**Phone Number:** e.g. *+12345678901* (E.164 format)  
**Human Name:** e.g. *"John Smith"* (must be in quotes)  
**Username:** e.g. *"jsmith2000"* (must be in quotes)  
**Network ASN:** e.g. *1234*

[By Use Case](#)[By Required Data](#)[By Module](#) All**Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

 Footprint**Understand what information this target exposes to the Internet.**

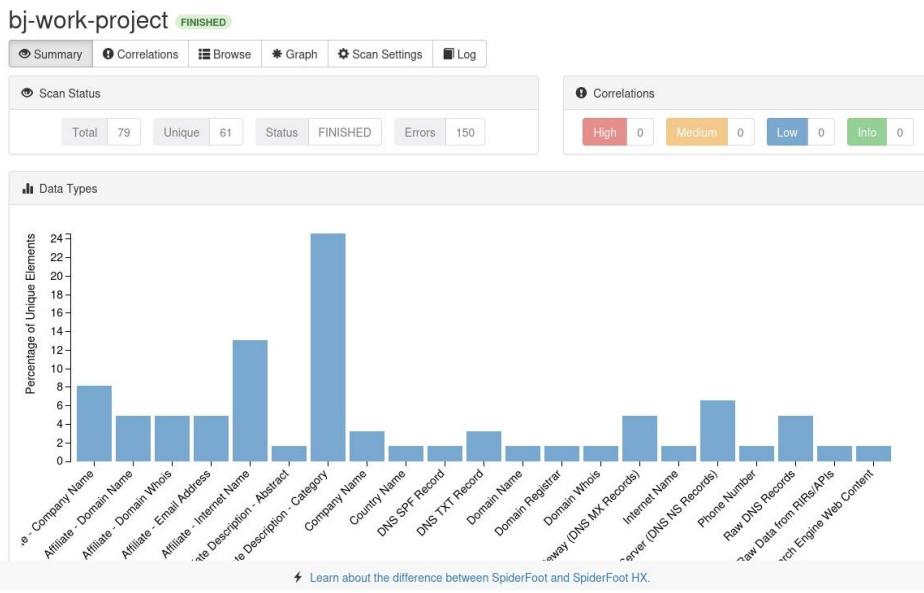
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

 Investigate**Best for when you suspect the target to be malicious but need more information.**

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

 Passive**When you don't want the target to even suspect they are being investigated.**

⚡ [Create a \(free\) SpiderFoot HX account](#) in seconds and try it out for yourself.



bj-work-project FINISHED

Summary Correlations Browse Graph Scan Settings Log

CSV

Search...

Q

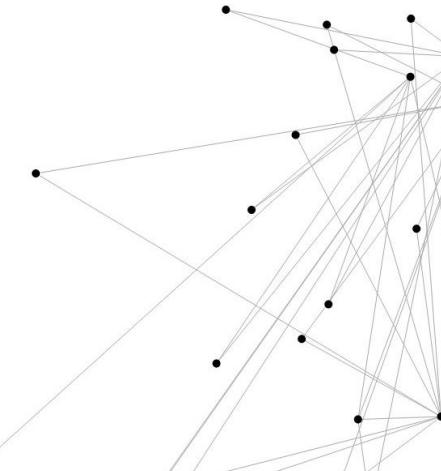
Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Company Name	5	9	2025-11-26 16:09:26
Affiliate - Domain Name	3	11	2025-11-26 16:08:45
Affiliate - Domain Whois	3	3	2025-11-26 16:09:26
Affiliate - Email Address	3	6	2025-11-26 16:09:27
Affiliate - Internet Name	8	8	2025-11-26 16:03:09
Affiliate Description - Abstract	1	1	2025-11-26 16:07:53
Affiliate Description - Category	15	15	2025-11-26 16:07:53
Company Name	2	2	2025-11-26 16:07:42
Country Name	1	4	2025-11-26 16:09:26
DNS SPF Record	1	1	2025-11-26 16:03:08
DNS TXT Record	2	2	2025-11-26 16:03:08
Domain Name	1	1	2025-11-26 16:03:07
Domain Registrar	1	1	2025-11-26 16:03:33
Domain Whois	1	1	2025-11-26 16:03:33
Email Gateway (DNS MX Records)	3	3	2025-11-26 16:03:08
Internet Name	1	1	2025-11-26 16:03:07

Learn about the difference between SpiderFoot and SpiderFoot HX.

## bj-work-project FINISHED

[Summary](#) [Correlations](#) [Browse](#) [Graph](#) [Scan Settings](#) [Log](#)

R F



⚡ Learn about the difference between SpiderFoot and SpiderFoot HX.

### Meta Information

Name:	bj-work-project
Internal ID:	3EB832F8
Target:	bjnetworksolution.xyz
Started:	2025-11-26 16:02:54
Completed:	2025-11-26 16:23:22
Status:	FINISHED

### Global Settings

Option	Value
Enable debugging?	0
Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.	
Number of seconds before giving up on a HTTP request.	5
List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics.	abuse,admin,billing,compliance,devnull,dns,ftp,hostmaster,iroc,ispfeedback,ispsupport,ist-request,list,maildaemon,marketing,noc,no-reply,no-reply,null,peering,peering-notify,peering-request,phish,phishing,postmaster,privacy,registrar,registry,root,routing-registry,rr,sales,security,spam,spam,sysadmin,tech,undisclosed-recipients,unsubscribe,usenet,uucp,webmaster,www
List of Internet TLDs.	<a href="https://publicsuffix.org/list/effective_tld_names.dat">https://publicsuffix.org/list/effective_tld_names.dat</a>
Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.	72

⚡ Learn about the difference between SpiderFoot and SpiderFoot HX.

## Scans

Filter: None

<input type="checkbox"/>	Name	Target	Started	Finished	Status	Elements	Correlations	Action
<input type="checkbox"/>	bj-work-project	bjnetworksolution.xyz	2025-11-26 16:02:53	2025-11-26 16:23:21	FINISHED	79	0  0  0 0	

Scans 1 - 1 / 1 (1)

## Recommendations (Based on Passive Posture Only)

1. **HTTP Security Headers:** Verify presence of [Strict-Transport-Security](#), [Content-Security-Policy](#), [X-Content-Type-Options](#), [Referrer-Policy](#), and [Permissions-Policy](#).